(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09073416 A**

(43) Date of publication of application: **18.03.97**

(51) Int. Cl **G06F 12/14**
B42D 15/10
B42D 15/10
G06K 19/073

(21) Application number: **07250120**

(22) Date of filing: **05.09.95**

(71) Applicant: **DAINIPPON PRINTING CO LTD**

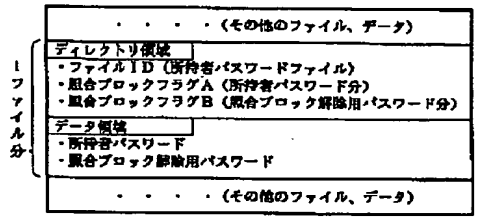
(72) Inventor: **HAYASHI MASAHIRO**

(54) **IC CARD**

(57) Abstract:

PROBLEM TO BE SOLVED: To actualize the state management of key data by increasing the memory use efficiency of the key data.

SOLUTION: This IC card has a plurality of relative key data stored in the data area of a key data file containing key data. The relative key data are, for example, a read authority password, a write control, authority password, and an issuer authority password as passwords for file access control. Further, a ciphering key and a deciphering key or an internal authorization key and an external authorization key used for mutual authorization between different IC cards are also mutually relative key data.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－73416

(43)公開日　平成９年(1997)３月18日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｃ	
				３２０Ｂ	
Ｂ４２Ｄ　15/10	５０１		Ｂ４２Ｄ　15/10	５０１Ｐ	
	５２１			５２１	
Ｇ０６Ｋ　19/073			Ｇ０６Ｋ　19/00	Ｐ	

審査請求　未請求　請求項の数４　ＦＤ　（全５頁）

(21)出願番号　特願平7－250120

(22)出願日　平成７年(1995)９月５日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　林　昌弘
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

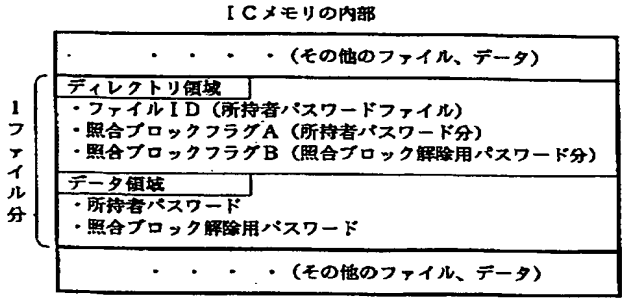
(74)代理人　弁理士　小西　淳美

(54)【発明の名称】　ＩＣカード

(57)【要約】

【課題】　キーデータのメモリ使用効率を上げ、キーデータの状態管理を実現する。

【解決手段】　キーデータを格納するキーデータファイルのデータ領域に、関連する複数のキーデータを格納したＩＣカードとする。関連する複数のキーデータとは、例えば、ファイルアクセス制御用のパスワードである、読取り権限パスワード、書込み権限パスワード、発行者権限パスワード等である。また、暗号化キーと復号化キー、或いは異なるＩＣカード間の相互認証用に用いる内部認証キーと外部認証キー等も相互に関連するキーデータである。



1

【特許請求の範囲】

【請求項１】　キーデータを格納するキーデータファイルのデータ領域に、関連する複数のキーデータを格納したことを特徴とするＩＣカード。

【請求項２】　関連する複数のキーデータが、ファイルアクセス制御用のパスワードとして、少なくとも読取り権限パスワード、書込み権限パスワード、発行者権限パスワードのうちの２以上のパスワードであることを特徴とする請求項１記載のＩＣカード。

【請求項３】　関連する複数のキーデータが、異なるＩＣカード間の相互認証用に用いる内部認証キーと外部認証キーであることを特徴とする請求項１記載のＩＣカード。

【請求項４】　関連する複数のキーデータが、暗号化キーと復号化キーであることを特徴とする請求項１記載のＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカードに関し、特にセキュリティ管理、メモリ効率及び処理効率が良いＩＣカードに関する。

【０００２】

【従来の技術】ＩＣカードは、記憶容量が大きく、セキュリティ性が高いなどと優れており今後が期待されている。ところで、ＩＣカードのセキセュリティ管理は、パスワード用キー、認証用キー、暗号化／復号化用キー等の各キーを用いて行っており、これらキーデータはそれぞれ内部基礎ファイルという形態に格納して使用される。パスワード用キーは、主にファイルアクセス制御に使われ、認証用キーは主に暗号認証に使われ、暗号化／復号化キーは主にデータの暗号化と復号化に使われている。なお、暗号化／復号化キーは例えば配送鍵の使用の際に使われる。

【０００３】これらの内部基礎ファイルのうち、通常もっとも利用されるのはファイルアクセス制御のためのパスワード用キーが格納されたファイルである。そこで、このパスワード用キーファイルを例に、従来のキーデータの使われ方を以下説明する。ＩＣカードに記憶されるデータのセキュリティ管理は、データをデータファイルに格納し、パスワード照合でアクセス権を獲得しないと該データファイルに対してアクセスできない仕組みにしてある。そして、一つのデータファイルの或るアクセスに要求されるパスワード（暗証番号）も、複数のパスワードを用い、またアクセスの形態、すなわち読み出し、書き込み、更新等によって、用いるパスワードを変える等して、データファイルに対するアクセス制御を行いセキュリティ性を確保している。また、パスワード照合で用いるパスワード用キーもデータの一種であり、一つのパスワード用キーファイルに一つのパスワード用キーが格納されており、パスワード用キーファイルもアクセス

2

制御の対象となるファイルである。

【０００４】そして、一般にファイルはディレクトリ領域とデータ領域から構成され、データ領域には記憶すべきデータやパスワード用キーが格納され、ディレクトリ領域にはそのファイルを識別するファイルＩＤ、その他の情報が格納される。内部基礎ファイルとしてパスワード用キーファイル等のキーファイルの場合には、図2に示すように、データ領域にはパスワード用のキーデータが格納され、ディレクトリ領域にはファイルＩＤの他に、パスワード照合最大エラー回数及びエラーカウンタ、さらにパスワード照合機能が実行できる状態であるか否かを示す照合ブロックフラグ等も格納されている。照合機能がブロックされて状態ではパスワード照合は実行不可能である。これは、誤ったパスワードでパスワード照合を繰り返すとパスワードエラーカウンタがカウントし、カウンタの値がパスワード照合最大エラー回数に達すると、照合ブロックフラグがセットされてブロック状態となり、以降のパスワード照合を受け付けなくするというものである。なお、或るデータファイルのファイルアクセス制御に使用するパスワード用キーファイルは、通常、別個のファイルに格納されたファイルアクセス制御テーブルによって定義されている。

【０００５】

【発明が解決しようとする課題】ところで、例えば上述のようなパスワード用キーファイルにおいて、パスワードのうち所持者パスワードについてパスワード照合に失敗して、パスワード照合の規定回数（最大エラー回数）をオーバーした場合、パスワード照合機能がブロックされ、以降そのパスワードを使用する動作は実行不可能となり、ＩＣカードは使用できなくなる。このＩＣカードを再使用できる様に戻すためには、ブロック状態を解除することが必要となるが、解除は特定の管理者のみしか行えない。この場合、ＩＣカードの発行元は、照合ブロック解除用のパスワードを新たにＩＣカードに設定する、すなわち照合ブロック解除用パスワードを格納する照合ブロック解除用パスワードファイルを新たに追加することが多い。そして、この照合ブロック解除用パスワードを用いて特定の管理者がブロック状態を解除して、再使用できる様にしている。なお、セキュリティ性の点からパスワードは上述した如く通常は複数使用されるが、なかでも上記照合ブロック解除用パスワード等の管理用パスワードは、第三者に不正に利用されないことが重要である。

【０００６】照合ブロック解除用パスワードファイルを新設すると、図３に示すように、新たにディレクトリ領域とデータ領域とから構成されるファイルが、ＩＣカードのメモリが、本来のデータ記憶以外の用途に消費される。なお、図３ではメモリ空間内を所持者パスワードファイルと照合ブロックパスワードファイルが占有し、これらファイルの上方及び下方のメモリ空間にはその為の

ファイルやデータによって占有されることを示している。所持者パスワードファイルのディレクトリ領域のファイルＩＤはそのファイルが所持者パスワードファイルである情報であり、照合ブロックフラグＡは所持者パスワードに関する照合機能のブロック状態を示し、データ領域には所持者パスワードが格納される。また、照合ブロック解除用パスワードファイルにも同様に、該ファイルを示すファイルＩＤと照合ブロック解除用パスワードに対する照合機能のブロック状態を示す照合ブロックフラグＢがディレクトリ領域に、またデータ領域には照合ブロック解除用パスワードが格納される。

【０００７】また、セキュリティ管理上、所持者パスワードファイルの照合ブロックフラグ（照合ブロックフラグＡ）と、該照合ブロックフラグの解除用の、照合ブロック解除用パスワードが格納された照合ブロック解除用パスワードファイル自身の照合ブロックフラグ（照合ブロックフラグＢ）とは、利用形態上では、相互に密接な関連がある。しかし、図３のように、それぞれ別々のファイルとして設定されていると両フラグの状態を管理すること、つまり、ＩＣカードのＯＳでチェックして管理することは困難である。なぜなら、両パスワードファイルのブロック状態の管理をＩＣカードのＯＳで実行するには、その前提としとＯＳで特定のパスワードファイルのブロック状態をチェックする機能が必要だからである。このチェック機能とは、パスワードファイルの検索やそのブロック状態のチェック等である。すなわち、通常のＩＣカードは、初期状態では、主ファイルと呼ばれるＩＣメモリ全体を管理するファイル内に、ＩＣカードの発行者が、必要とするファイルを順次追加して設定することを前提に設計されている。したがって、上記ブロック状態の管理をＯＳで行うには、①ＯＳ上で２つのファイルを検索・チェックする機能と、②発行時においてこの２つのファイルを関連するファイルとして設定しておくことが必須となる。或いは、解除用パスワードファイルを後で設定する場合は、未設定の解除用パスワードファイルを（既設定の）パスワードファイルと関連するファイルとしてＯＳで管理できることが必要となる。

【０００８】

【課題を解決するための手段】本発明のＩＣカードの第１の発明は、キーデータを格納するキーデータファイルのデータ領域に、関連する複数のキーデータを格納した構成とする。また、本発明のＩＣカードの第２の発明は、上記第１の発明のＩＣカードにおいて、関連する複数のキーデータが、ファイルアクセス制御用のパスワードとして、少なくとも読取り権限パスワード、書込み権限パスワード、発行者権限パスワードのうちの２以上のパスワードである構成とする。また、本発明のＩＣカードの第３の発明は、前記第１の発明のＩＣカードにおいて、関連する複数のキーデータが、異なるＩＣカード間の相互認証用に用いる内部認証キーと外部認証キーである構成とする。また、本発明のＩＣカードの第４の発明は、前記第１の発明のＩＣカードにおいて、関連する複数のキーデータが、暗号化キーと復号化キーである構成とする。

【０００９】

【発明の実施の形態】以下、本発明のＩＣカード実施の形態を図面を参照しながら、幾つかの実施例をもとに説明する。

【００１０】先ず、本発明のＩＣカードでは、関連するキーデータを一つのキーデータファファイル（内部基礎ファイル）のキーデータ領域に格納する点に特徴があり、以下説明するように密接に関連するキーデータを一ファイル中にまとめて格納することが好ましい。また、キーデータファイルの場合には、キーデータの照合機能に関する照合ブロックフラグ等もファイルのディレクリ領域にあるので、一ファイルにまとめて格納するキーデータ毎の照合ブロックフラグもディレクトリ領域にまとめて格納することで、これら関連するキーデータ及び照合ブロックフラグの管理、及びこれらを使用する各種処理が効率的に行える。

【００１１】先ず、図１は、キーデータとして、所持者パスワードと、所持者パスワードの照合ブロックフラグに対する照合ブロックフラグ解除用パスワードとを、一つのファイルにまとめた場合の、ＩＣメモリ内のファイル内容を概念的に説明する説明図である。図１の例では、一つにまとめたファイル名、すなわちファイルＩＤは所持者パスワードファイルであり、照合ブロック解除用パスワードを所持者パスワードファイルにまとめたものである。その結果、同図に示す如く、データ領域には、相互に関連する所持者パスワードと（該所持者パスワードの照合機能がブロックした時にブロックを解除するための）照合ブロック解除用パスワードとが格納される。また、ディレクトリ領域には、所持者パスワードファイルと識別するファイルＩＤと、所持者パスワードに対する照合ブロックフラグＡとともに、照合ブロックフラグ解除用パスワードに対する照合ブロックフラグである照合ブロックフラグＢとが、同一のディレトリ内にまとめてあるので、ＩＣカードのＯＳでの管理チェックも容易となる。なお、図１のディレクト領域内には、これら以外に図２に示した、パスワード照合最大エラー回数及びエラー・カウンタ等もそれぞれのパスワード毎に格納される。また、図１の所持者パスワードとその照合ブロック解除用パスワードとをまとめたファイルは、図３のそれぞれのパスワードを独立のファイルに格納した従来のファイル使用方法に対応する。このように図１に示すようにデータ領域に格納する複数のキーデータのそれぞれに対応する複数の照合ブロックフラグを一つのディレクトリ領域に格納することで、メモリ容量が節約される。

【００１２】次の本発明のＩＣカードのキーデータファ

5

イルの一実施例は、図４に示す如くデータファイルに対するアクセス制御用のキーデータを一つのファイルにまとめたものである。図４の例では、読取り用パスワードと、書込み用パスワードと、発行者用パスワードとが一つのファイルとして、データアクセスパスワードファイルのデータ領域に格納してある。なお、同図ではディレクトリ領域には、ファイルＩＤのみを明示してあるが、図２に示したように、各パスワード毎にパスワード照合最大エラー回数及びエラー・カウンタ、照合ブロックフラグ等もディレクトリ領域に格納されている。

【００１３】また、図５は本発明の他の実施例におけるキーデータファイルの内容を示すものであり、同図では相互に関連するＩＣカードＡ及びＩＣカードＢという２枚のＩＣカードにおいて、内部認証用キーと外部認証用キーとを（各ＩＣカード毎に）一つの相互認証用キーファイルにまとめたものである。ＩＣカードＡ及びＢのそれぞれに、内部認証用キーと外部認証用キーとが格納されている。なお、相互認証とは、Ａ（以下、ＩＣカードＡ）とＢ（以下、ＩＣカードＢ）とで、お互いの正当性を証明する方法である。そして暗号を利用する相互認証にて、上記の内部認証用キーと外部認証用キーは暗号鍵として使用される。つまり、ＡとＢとが、同じ「暗号アルゴリズム〔例えばＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）やＦＥＡＬ（Ｆａｓｔ Ｄａｔａ Ｅｎｃｉｐｈｅｒｍｅｎｔ Ａｌｇｏｒｉｔｈｍ）など〕」と「暗号鍵」を持っていれば、「同じ数値」の暗号計算で、「同じ結果」を出力する。相互認証では、両方で同一の乱数を交換し、この２つの暗号計算の結果を互いに照合して、その正当性の認証を行う。Ｂの正当性を（Ａに対して）証明する場合、Ａの外部認証キーとＢの内部認証キーが利用される。すなわち、Ａで生成した乱数がＢに送信され、Ｂは受信した乱数による計算を内部認証キーで行いその計算結果をＡに送信する。Ａでは送信する乱数による計算を外部認証キーで行いその計算結果をＢから送信された計算結果と比較照合する。同様に、Ａの正当性を証明するには、Ａの内部認証用キーとＢの外部認証用キーが利用され、Ｂで生成した乱数がＡに送信され、Ａは計算結果をＢに送信する。このようにして、ＡとＢでは２つの暗号鍵（外部認証キーと内部認証キー）を利用する。

【００１４】また、図６も本発明の他の実施例におけるキーデータファイルの内容を示すものであり、同図で

6

は、ＩＣカードＡとＩＣカードＢとで暗号化と復号化を行うＩＣカードである。相互に関連するＩＣカードA及びＩＣカードＢという２枚のＩＣカードにおいて、暗号化キーと復号化キーとを（各ＩＣ毎に）一つの暗号化関連キーファイルとしてまとめたものである。ＩＣカードＡ及びＢのそれぞれに、暗号化キーと復号化キーとが格納されている。なお、これらキーは、例えばＩＣカードＡの暗号化キーで或る情報を暗号化してＩＣカードＢに渡し、ＩＣカードＢでは暗号化された情報を復号化キーで復号化して元の情報に戻す。また、逆にＩＣカードＢからＩＣカードＡへもＩＣカードＢで暗号化してＩＣカードＡで復号化する。

【００１５】上記の如く、関連するキーデータの組み合わせとしては各種のものがあるが、本発明の関連するキーデータ及びその組み合わせ方は、これらに限定されるものではない。また、上記の様に、関連するキーデータを一つのファイル・ディレクトリ領域で管理できるため、ＯＳで同時に２つのファイルの状態を参照する必要がなくなり、ファイルの処理およびメモリ効率において有利である。

【００１６】

【発明の効果】本発明のＩＣカードによれば、一つのキーデータファイルに関連するキーデータをまとめて格納するので、メモリの使用効率、セキュリティ管理、処理効率が向上する。

【図面の簡単な説明】

【図１】本発明のＩＣカードの一実施例におけるキーデータファイルを示す説明図。

【図２】ＩＣカードのメモリ内におけるキーデータを格納する内部基礎ファイルのファイル構造を示す説明図。

【図３】従来のＩＣカードにおけるメモリ消費を説明する説明図。

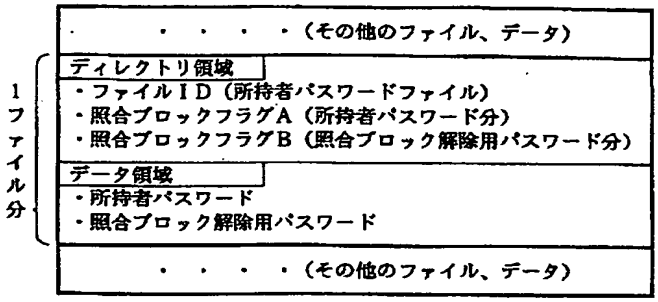
【図４】本発明のＩＣカードの他の実施例における、関連するキーデータ（アクセス制御用キーデータ）を示す説明図。

【図５】本発明のＩＣカードの他の実施例における、関連するキーデータ（相互認証用キーデータ）を示す説明図。

【図６】本発明のＩＣカードの他の実施例における、関連するキーデータ（暗号化関連キーデータ）を示す説明図。

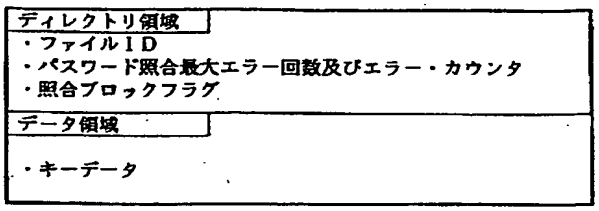
【図１】

ＩＣメモリの内部



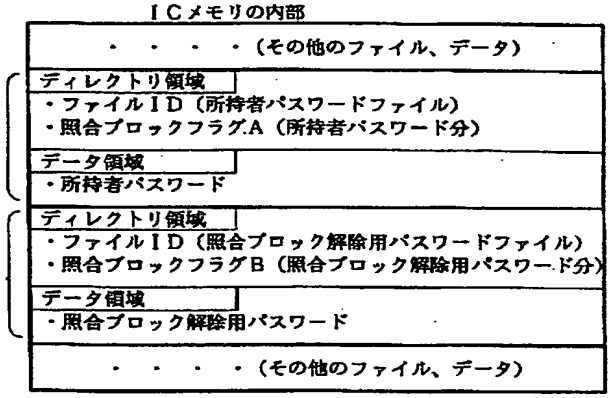
【図２】

ファイルの構造



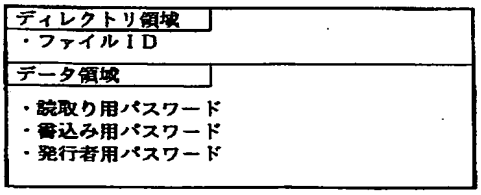
【図３】

ＩＣメモリの内部



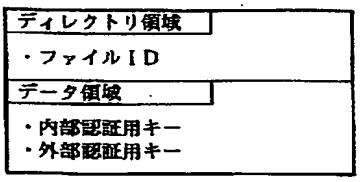
【図４】

データアクセスパスワードファイル

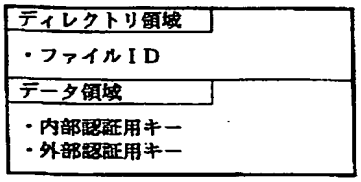


【図５】

ＩＣカードＡ：
相互認証用キーファイル

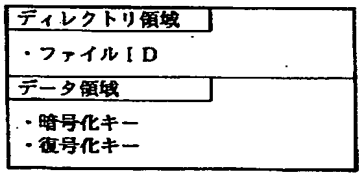


ＩＣカードＢ：
相互認証用キーファイル



【図６】

ＩＣカードＡ：
暗号化関連キーファイル



ＩＣカードＢ：
暗号化関連キーファイル